Province of the
EASTERN CAPE
EDUCATION

Directorate IT & SI

E-Mail Acceptable Use Policy

Status:	In draft Under Review Sent for Approval Approved Rejected	
Version:	V1.0	
Release Date:	10.04.2016	

A. FOREWORD

This document sets out the E-MAIL ACCEPTABLE USE POLICY and procedures to be followed within the Eastern Cape Department of Education with respect to the important functions related to the management of information technology. This also covers schools and other ECDoE subsidiaries.

This policy is a living document and may be amended at any time. Any questions regarding this policy should be directed to Director: IT&SI.

Additional policies will be developed as the need arises. It is important for all staff who use computers in any form to be familiar with this policy.

B. DOCUMENT OWNERSHIP

The Department reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately. A copy of the latest version may be obtained from:

The office of the Director: Information Technology and Systems Infrastructure
Department of Education
Head Office Park, Steve Tshwete Complex
Zone 6,
Zwelitsha

C. REVISION CONTROL

Version	Date
V1.0	10 April 2016

D. ABBREVIATIONS AND DEFINITIONS

The following abbreviations and definitions are used in this document:

AG	Auditor-General
Data message	In terms of section 1 of the Electronic Communications and Transactions Act (Act No. 25 of 2002) " 'data message' means data generated, sent, received or stored by electronic means and includes: (a) voice, where the voice is used in an automated transaction; and (b) a stored record." Part (b) includes emails.
ECDoE	Eastern Cape Department of Education
DGITO	Departmental Government Information Technology Officer
Electronic Communication System	This comprises the local area network (LAN) and its components, email, fax machines and telephone systems.
FTP	File Transfer Protocol.
GITO	Government Information Technology Officer
GPO	Directory and Group Policy Object.
HTML	Hypertext Mark-up Language.
HTTP	Hypertext Transfer Protocol.
ICT	Information and Communications Technology
IP	Internet Protocol.
ISA	Internet Security Accelerator.
IT	Information Technology
PFMA	Public Finance Management Act
PGITO	Provincial Government Information Technology Officer
SIGNED CODE	Code signing is a mechanism whereby publishers of software and content can use a certificate-based digital signature to verify their identities to users of the code, thus allowing users to decide whether or not to install it based on whether they trust the publisher.
SITA	State Information Technology Agency
SI	Systems Infrastructure
SLA	Service Level Agreement
SMS	Short Message Service on cellular networks or via Internet Service Providers.
SMTP	Send Mail Transfer Protocol.
Software	All computer programs and code, commercial or otherwise, that is installed on a single, stand-alone computer, or network server, or a workstation connected to a network server. The list of installed software for each computer can be viewed by clicking on Start, then select Control Panel, then click on the Add/Remove Programs option.
SUS	Microsoft Software Upgrade Services.

System data	All installed software and settings that have been saved via the Operating System (OS) (normally Microsoft Windows or Novell on the networks and servers) including all definition files, registry settings, security information and other data that is used by a software program or the operating system.
TCP	Transmission Control Protocol.
UDP	User Datagram Protocol.
URL	Uniform Resource Locator.
User data	Includes all data that has been stored on a computer by the user of a software program that contains working information such as spreadsheets, documents, presentations, etc.
VPN	Virtual Private Network.
MAC	Moves, Additions and Changes

1) Purpose

- E-mail is a critical mechanism for business communications at ECDoE. However, use of ECDoE's electronic mail systems and services are a privilege, not a right, and therefore must be used with respect and in accordance with the goals of ECDoE.

- The objectives of this policy are to outline appropriate and inappropriate use of ECDoE's e-mail systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

2) Scope

- This policy applies to all e-mail systems and services owned by ECDoE, all e-mail account users/holders at ECDoE (both temporary and permanent), and all the department's e-mail records.

3) Account Activation/Termination

- E-mail access at ECDoE is controlled through individual accounts and passwords. Each user of ECDoE's e-mail system is required to read a copy of this E-mail Acceptable Use Policy when issued with an e-mail access account and password. It is the responsibility of the employee to protect the confidentiality of their account and password information.

- All employees of ECDoE will receive an e-mail account. E-mail accounts will be granted to third-party non-employees on a case-by-case basis. Possible non-employees that may be eligible for access include:
  - Contractors.
  - Temporary workers.
  - Interns.
- Applications for these temporary accounts must be submitted to the Service Desk at IT offices. All terms, conditions, and restrictions governing e-mail use must be in a written and signed document.

- E-mail access will be terminated when the employee or third party terminates their association with ECDoE.

- ECDoE is under no obligation to store or forward the contents of an individual's e-mail inbox/outbox after the term of their employment has ceased.

4) General Expectations of End Users

- The department often delivers official communications via e-mail. As a result, employees of ECDoE with e-mail accounts are expected to check their e-mail in a consistent and timely manner so that they are aware of important departmental announcements and updates, as well as for fulfilling business and role-oriented tasks.

- E-mail users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, he or she must be aware of how to unsubscribe from the list, and is responsible for doing so in the event that their current e-mail address changes.

- E-mail users are expected to remember that e-mail sent from the department's e-mail accounts reflects on the department. Please comply with normal standards of professional and personal courtesy and conduct.

5) Appropriate Use

- Individuals at ECDoE are encouraged to use e-mail to further the goals and objectives of ECDoE. The types of activities that are encouraged include:
  - Communicating with fellow employees, business partners of ECDoE, and clients within the context of an individual's assigned responsibilities.
  - Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
  - Participating in educational or professional development activities.

6) Inappropriate Use

- ECDoE's e-mail systems and services are not to be used for purposes that could be reasonably expected to strain storage or bandwidth (e.g. e-mailing large attachments instead of pointing to a location on a shared drive). Individual e-mail use will not interfere with others' use and enjoyment of ECDoE's e-mail system and services. E-mail use at ECDoE will comply with all applicable laws, all ECDoE policies, and all ECDoE contracts.

- The following activities are deemed inappropriate uses of ECDoE e-mail systems and services, and are strictly prohibited:
  - Use of e-mail for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
  - Viewing, copying, altering, or deletion of e-mail accounts or files belonging to ECDoE or another individual without authorized permission.
  - Sending of unreasonably large e-mail attachments. The total size of an individual e-mail message sent (including attachment) should be 5MB or less.
  - Opening e-mail attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
  - Sharing e-mail account passwords with another person, or attempting to obtain another person's e-mail account password. E-mail accounts are only to be used by the registered user.
  - Excessive personal use of ECDoE e-mail resources. ECDoE allows limited personal use for communication with family and friends, independent learning, and public service so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources. ECDoE prohibits personal use of its e-mail

systems and services for unsolicited mass mailings, non-ECDoE commercial activity, political campaigning, dissemination of chain letters, and use by non-employees.

7) Monitoring and Confidentiality

- The e-mail systems and services used at ECDoE are owned by the ECDoE and are therefore its property. This gives ECDoE the right to monitor any and all e-mail traffic passing through its e-mail system. This monitoring may include, but is not limited to, inadvertent reading by IT staff during the normal course of managing the e-mail system, review by the legal team during the e-mail discovery phase of litigation, observation by management in cases of suspected abuse or to monitor employee efficiency.

- In addition, archival and backup copies of e-mail messages may exist, despite end-user deletion, in compliance with ECDoE's records retention policy. The goals of these backup and archiving procedures are to ensure system reliability, prevent business data loss, meet regulatory and litigation needs, and to provide business intelligence.

- Backup copies exist primarily to restore service in case of failure. Archival copies are designed for quick and accurate access by ECDoE delegates for a variety of management and legal needs. Both backups and archives are governed by the ECDoE's document retention policies. E-mail must be kept for up to 5 years. If ECDoE discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, e-mail records may be retrieved and used to document the activity in accordance with due process. All reasonable efforts will be made to notify an employee if his or her e-mail records are to be reviewed. Notification may not be possible, however, if the employee cannot be contacted, as in the case of employee absence due to vacation.

- Use extreme caution when communicating confidential or sensitive information via e-mail. Keep in mind that all e-mail messages sent outside of ECDoE become the property of the receiver. A good rule is to not communicate anything that you wouldn't feel comfortable being made public. Demonstrate particular care when using the "Reply" command during e-mail correspondence to ensure the resulting message is not delivered to unintended recipients.

8) Reporting Misuse

- Any allegations of misuse should be promptly reported to IT Service Desk offices at 040 608 4252 or email to itsupport@edu.ecprov.gov.za. If you receive an offensive e-mail, do not forward, delete, or reply to the message. Instead, report it directly to the office named above.

9) Disclaimer

"Eastern Cape Department of Education(ECDoE) assumes no liability for direct and/or indirect damages arising from the user's use of ECDoE's e-mail system and services. Users are solely responsible for the content they disseminate. ECDoE is not responsible for any third-party claim, demand, or damage arising out of use the ECDoE's e-mail systems or services."

10) Management

Ownership of this policy falls to Dir.: IT&SI. For any questions about this policy please contact him/her at 040-6084244.

11) Revision

IT Management is responsible for keeping this policy current. This policy will be reviewed annually or as circumstances arise.

An internal audit will be performed annually to ensure that the policy is properly aligned with ECDoE objectives and that performance is meeting established triage parameters.

12) Enforcement

It is the responsibility of all managers of operating units to ensure that these policies are clearly communicated, understood and followed by the staff for whom they are responsible.

Any user or staff member found to have violated this policy may be subject to:

Disciplinary action as described in the Department's Code of Conduct and Disciplinary Procedures including revocation of his/her computer account, suspension, or termination of employment, or Civil or Criminal prosecution.

APPROVAL

This document was recommended by the DGITO and approved by the Acting Superintendent General.

B Khohliso
Director: IT & SI

16/09/2016
Date

GF Mac Master
Acting Superintendent General

16/09/2016
Date

ISEBE LEMFUNDO NENKCUBEKO
IPHONDO LEMPUMA KOLONI
DEPARTMENT OF EDUCATION
2016 -09- 16
PROVINCE OF THE EASTERN CAPE
OOS-KAAP PROVINSIE